UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/568,207	06/04/2008	Christopher John Burke	SECU-PCT-US-1	8109

757 7590 08/25/2009

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

EXAMINER	
RAHMAN, MOHAMMAD L	
ART UNIT	PAPER NUMBER
2438	
MAIL DATE	DELIVERY MODE
08/25/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/568,207	BURKE, CHRISTOPHER JOHN	
	Examiner	Art Unit	
	MOHAMMAD L. RAHMAN	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 May 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *48-64* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *48-64* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02/13/2006,03/28/2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04/16/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Preliminary Amendment

The Preliminary amendment filed 05/04/2009 received and acknowledged. Claims 1-47 have been canceled. New claims 48-64 have been added. Pursuant to U.S.C. § 119 and 37 C.F.R. § 1.55, claims 48-64 presented for examination. Claims 48-64 are pending. At this time, claims 48-64 are rejected.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).The certified copy has been filed in parent Application No. PCT/AU2004/001083, filed on 03/28/2008.

Information Disclosure Statement

The information disclosure statement filed 04/16/2009 has been placed in the application file and the information referred to therein have been considered as to the merits.

Oath/Declaration

The Oath filed on 06/04/2008 complies with all the requirements set forth in MPEP 602 and therefore is accepted.

Drawings

The drawings filed on 02/13/2006 and 03/28/2008 has been accepted.

Claim Objections

Claims 53-60, 62 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or

rewrite the claim(s) in independent form. Claims recited that above claims are dependent on claims 5, 6, 7,1,12, 14 which do not exist.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 51, 64 rejected under 35 U.S.C. 101 because they are directed to non-statutory subject matter as failing to fall within a statutory category of invention.

Claims **51, 64** directed to program per se as the preamble of the claim clearly recites "a computer program product". Further, claims 51, 64 directed to signal per se. The preamble of the claim recites "a computer program product having a computer readable medium" but in the specification on page 28, lines 1-10, the applicants' has defined "the computer readable medium as used herein refers to *any storage or transmission medium* that participates in providing instructions and/or data to the transmitter sub-system." Further, "Examples of transmission media include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the internet or intranets" It is clearly recited that computer instructions is provided as signals embodied in a carrier wave medium which is non-statutory. "A transitory, propagating signal ... is not a "process, machine, manufacture, or composition of matter." Those four categories define the explicit scope and reach of subject matter patentable under 35 U.S.C. 101; thus, such a signal cannot be patentable subject matter." (In re Petrus A.C.M. Nuijten; Fed Cir, 2006-1371, 9/20/2007). Because the full scope of claim 51, 64 as properly read in light of the disclosure encompasses non-statutory subject matter (i.e., because the limitation "a computer-readable medium" would include a non-statutory signal,

carrier wave, etc.), claims 51, 64 are rejected under 35 U.S.C. 101 for reciting non-statutory subject matter.

Claims 49, 61 rejected under 35 U.S.C. 101 because they are directed to non-statutory subject matter as failing to fall within a statutory category of invention.

Claims 49 and 61 recites in the preamble "A transmitter sub-system" that the claims are directed towards category of a system. However, the body of the claims comprises a series of "logic" and this is directed towards functional descriptive material. Therefore, it is not clear how a series of "logic" (or functional descriptive material) constitutes a system. Further, specification disclosed (Page 27, lines 19-21), "the application program modules for the transmitter sub-system". Therefore, application program module for the transmitter subsystem clearly directed towards system software per se, non-statutory. Clarification required. For examination purposes, Examiner has construed the system contain a combination of software and hardware elements.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 48, 49, 52, 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Martin et al. WO 01/71462 (hereinafter "Martin") in view of Hoffman et al. US 7,152,045 (hereinafter "Hoffman").

Regarding claim 48, Martin taught a system for providing secure access to a controlled item (*see [Abstract] a system and method for secure biometric identification which includes a mobile*

unit and a server. The mobile unit is adapted to receive biometric input; the server is equipped for authenticating the biometric data and providing second signal to the mobile unit where it is utilized to access the secure device. e.g., encrypted database), the system comprising:

a transmitter subsystem for enrolling biometric signatures into a database and for providing an accessibility attribute (*see the reason for obviousness*) if a legitimate biometric signal is received (*see [Page 4, lines 16-24; fig. 2] the mobile unit subsystem as transmitter subsystem includes wireless transceiver, CPU receives biometric data from the fingerprint sensor for providing access to a secure device [Page 6, lines 10-16 if a match is achieved [Page 5, lines 22-23]*); and

a receiver sub-system (*see [fig. 3, page 4, lines 32-36] a server subsystem as receiver sub system for secure biometric identification and when a match is achieved, [5/22-24] a user is identified and an authentication key specific to the identified mobile user is retrieved and transmitted back to mobile unit to gain access [6/10-20] to a secure device*) for providing access to the controlled item dependent upon said accessibility attribute (*see the reason for obviousness below*).

Martin taught the system in claim 1; Martin was silent on accessibility attribute and providing access to the controlled item dependent upon said accessibility attribute. However, Hoffman taught accessibility attribute and providing access to the controlled item dependent upon said accessibility attribute (*see [Col. 40, lines 62-67] the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute])*

Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the invention of Martin with the teachings of Hoffman for the use

of providing access to the item based on accessibility attribute because they are analogous in biometric identification, authentication, and authorization.

One of ordinary skill in the art would have been motivated to incorporate the idea of providing access to the item based on accessibility attribute of Hoffman *[Col. 40, lines 62-67, Col. 41, lines 1-8]* within the system of Martin [*Fig. 4(a)-4(c)*] because the idea of Hoffman could provide the system of Martin the ability to an authorized user to alert authorities that a third party is coercing the user to request access without the third party being aware that an alert has been generated (*Hoffman, Col. 5, lines 62-67*)

Regarding claim 49, the combination of Martin and Hoffman further taught

a transmitter sub-system [*Martin, fig. 2*] adapted for operation in a system for providing secure access to a controlled item, the system further including

a receiver sub-system for providing access to the controlled item dependent upon an accessibility attribute *[Hoffman, Col. 40, lines 62-67, Col. 41, lines 1-8]* received from the transmitter sub-system (*see [fig. 3, page 4, lines 32-36] a server subsystem as receiver sub system for secure biometric identification and when a match is achieved, [5/22-24] a user is identified and an authentication key specific to the identified mobile user is retrieved and transmitted back to mobile unit to gain access [6/10-20] to a secure device*) ; wherein the a transmitter subsystem comprises:

means for enrolling biometric signatures into a database (*Hoffman, see [Col. 8, lines 35-40] storage of the entered biometric sample from first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample*); and

means for providing the accessibility attribute if a legitimate biometric signal is received (*Hoffman, see [Col. 40, lines 62-67] the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]*).

Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the invention of Martin with the teachings of Hoffman for the use of enrolling biometric signatures into a database and providing access to the item based on accessibility attribute because they are analogous in biometric identification, authentication, and authorization.

One of ordinary skill in the art would have been motivated to incorporate the idea of enrolling biometric signatures into a database [*Hoffman, see [Col. 8, lines 35-40]* and providing access to the item based on accessibility attribute of Hoffman *[Col. 40, lines 62-67, Col. 41, lines 1-8]* within the system of Martin [*Fig. 4(a)-4(c)*] because the idea of Hoffman could provide the system of Martin the ability to an authorized user to alert authorities that a third party is coercing the user to request access without the third party being aware that an alert has been generated (*Hoffman, Col. 5, lines 62-67*).

Regarding claim 52, the combination of Martin and Hoffman further taught a system for providing secure access to a controlled item (*Martin, see [Abstract] a system and method for secure biometric identification which includes a mobile unit and a server. The mobile unit is adapted to receive biometric input; the server is equipped for authenticating the biometric data and providing second signal*

to the mobile unit where it is utilized to access the secure device. e.g., encrypted database), the system comprising:

a database of biometric signatures [*Martin, fig. 3, item 54; Hoffman, fig. 2, item IBD*];

a transmitter subsystem [*Martin, fig. 2*] comprising:

a biometric sensor [*Martin, fig.2, item 28*] for receiving a biometric signal [*Martin, Page 4, lines 20-22*];

means for matching the biometric signal against members of the database of biometric signatures (*Martin, see [Page 5, lines 16-20] the decrypted fingerprint is compared by fingerprint matching software to a database of biometric data i.e. fingerprints*) to thereby output an accessibility attribute *[Hoffman, Col. 40, lines 62-67, Col. 41, lines 1-8]*;

means for emitting a secure access signal conveying information (*Martin, see [Page 5, lines 22-25], when a match is achieved, [5/22-24] a user is identified and an authentication key specific to the identified mobile user is retrieved and transmitted back to mobile unit to gain access [6/10-20] to a secure device)* dependent upon said accessibility attribute; and

means for enrolling biometric signatures into the database (*Hoffman, see [Col. 8, lines 35-40] storage of the entered biometric sample from first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample*); and

a receiver sub-system comprising [*Martin, fig. 3*];

means for receiving the transmitted secure access signal (*Martin, see [fig. 3, page 4, lines 32-36] a server subsystem as receiver sub system for secure biometric*); and

means for providing access to the controlled item dependent upon said information (*Hoffman, see [Col. 40, lines 62-67] the Data processing center (DPC) validates the biometric-PIC and*

sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]).

Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the invention of Martin with the teachings of Hoffman for the use of enrolling biometric signatures into a database and providing access to the item based on accessibility attribute because they are analogous in biometric identification, authentication, and authorization.

One of ordinary skill in the art would have been motivated to incorporate the idea of enrolling biometric signatures into a database [*Hoffman, see [Col. 8, lines 35-40]* and providing access to the item based on accessibility attribute of Hoffman *[Col. 40, lines 62-67, Col. 41, lines 1-8]* within the system of Martin [*Fig. 4(a)-4(c)*] because the idea of Hoffman could provide the system of Martin the ability to an authorized user to alert authorities that a third party is coercing the user to request access without the third party being aware that an alert has been generated (*Hoffman, Col. 5, lines 62-67*).

Regarding claim 61, the combination of Martin and Hoffman further taught

a transmitter subsystem [*Martin, fig. 2*] adapted for operating in a system for providing secure access to a controlled item (*see [Abstract] a system and method for secure biometric identification which includes a mobile unit and a server. The mobile unit is adapted to receive biometric input; the server is equipped for authenticating the biometric data and providing second signal to the*

mobile unit where it is utilized to access the secure device. e.g., encrypted database), the system comprising

a database of biometric signatures [*Martin, fig. 3, item 54; Hoffman, fig. 2, item IBD*], said transmitter subsystem, and a receiver sub-system comprising

means for receiving a transmitted secure access signal (*Martin, see [fig. 3, page 4, lines 32-36] a server subsystem as receiver sub system for secure biometric*), and

means for providing access to the controlled item dependent upon information in said secure access signal (*Hoffman, see [Col. 40, lines 62-67] the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]*), said transmitter sub-system comprising:

a biometric sensor [*Martin, fig.2 , item 28*] for receiving a biometric signal *Martin, Page 4, lines 20-22*];

means for emitting a secure access signal capable of granting access to the controlled item (*Martin, see [Page 5, lines 22-25], when a match is achieved, [5/22-24] a user is identified and an authentication key specific to the identified mobile user is retrieved and transmitted back to mobile unit to gain access [6/10-20] to a secure device)*; and

means for enrolling said biometric signatures into the database. (*Hoffman, see [Col. 8, lines 35-40] storage of the entered biometric sample from first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample*).

Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the invention of Martin with the teachings of Hoffman for the use of enrolling biometric signatures into a database and providing access to the item based on accessibility attribute because they are analogous in biometric identification, authentication, and authorization.

One of ordinary skill in the art would have been motivated to incorporate the idea of enrolling biometric signatures into a database [*Hoffman, see [Col. 8, lines 35-40]* and providing access to the item based on accessibility attribute of Hoffman *[Col. 40, lines 62-67, Col. 41, lines 1-8]* within the system of Martin [*Fig. 4(a)-4(c)*] because the idea of Hoffman could provide the system of Martin the ability to an authorized user to alert authorities that a third party is coercing the user to request access without the third party being aware that an alert has been generated (*Hoffman, Col. 5, lines 62-67*).

Claim 62-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffman in view of Martin and in further view of Koo et al., WO 02/12660 (hereinafter "Koo")

Regarding claim 62, Hoffman in view of Martin taught a transmitter sub-system according to claim 14 (examiner assume claim 61 for examination purpose), Hoffman in view of Martin was silent on, wherein the means for enrolling said biometric signatures into the database comprises: means for storing the biometric signal received by the biometric sensor in the database as an administrator signature if the database of biometric signatures is empty; means for, if an administrator signature has been stored in the database, classifying a legitimate sequence of biometric signals, each matching the administrator signature, as control information; and means for performing at least one of (a) amending information stored in the database

depending upon the control information, and (b) classifying a subsequent biometric signal as one of an administrator signature and an ordinary signature depending upon the control information.

However Koo taught

means for storing the biometric signal received by the biometric sensor in the database as an administrator signature if the database of biometric signatures is empty (*Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists as empty, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14*);

means for, if an administrator signature has been stored in the database, classifying a legitimate sequence of biometric signals, each matching the administrator signature, as control information (*Koo, see the person having inputted his fingerprint is authorized as a new administrator [Page 16, lines 12-15]; and see also [Page 11, lines 16-18] the fingerprint code of the administrator is stored by receiving the code stored in the administration system*); and

means for performing at least one of (a) amending information stored in the database depending upon the control information (*Koo, see [Page 17, lines 1-5] the door lock device recognizes a new user and erases all information related to the corresponding previous card key and changes as amended the initialization completion code*), and (b) classifying a subsequent biometric signal as one of an administrator signature and an ordinary signature depending upon the control information (*Koo, see [Page 16, lines 10-17, the fingerprint signature is registered as administrator and see also [Page 17, lines 22-25; 18/1-3] fingerprint code is registered as the initial user fingerprint code*).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the applicant's invention was made to modify the method of Hoffman with the teaching of Koo for storing biometric signal as an administrator signature and enabling administrative processing of

information stored in the database if a biometric signal matching the stored administrator signature is received by the transmitter because they are analogous in biometric entry.

One of ordinary skilled in the art would have been motivated to incorporate the idea of Koo *[Page, 5, lines 19-22; Page 16, lines 8-10]* within the method of Hoffman [fig. 1] because the idea of Koo could provide the method of Hoffman to provide an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (*Koo, Page 3, lines 21-23*).

Regarding claim 63, 64, the combination of Martin, Hoffman, and Koo further taught a method of/ a computer program product having a computer program product recorded therein [*Hoffman, Col. 13, lines 51-60*] for directing a processor to execute a method for enrolling, by a transmitter sub-system [*Hoffman, Col. 12, lines 50-55, Col. 13, lines 2-5, fig. 1 and 3*], biometric signatures into a database of biometric signatures in a system for providing secure access to a controlled item (*see [Col. 8, lines 35-40] storage of the entered biometric sample from first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample*),

the system comprising

(a) said database of biometric signatures [*Martin, fig. 3, item 54; Hoffman, fig. 2, item IBD*],

(b) the transmitter subsystem comprising a biometric sensor [*Martin, fig.2 , item 28*] for receiving a biometric signal [*Martin, Page 4, lines 20-22*],

means for emitting a secure access signal capable of granting access to the controlled item (*Martin, see [Page 5, lines 22-25], when a match is achieved, [5/22-24] a user is identified and an authentication key specific to the identified mobile user is retrieved and transmitted back to mobile unit to gain access [6/10-20] to a secure device)*and

means for enrolling said biometric signatures into the database (*Hoffman, see [Col. 8, lines 35-40] storage of the entered biometric sample from first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample*), and

(c) a receiver sub-system [Martin, fig. 3] comprising

means for receiving the transmitted secure access signal (*Martin, see [fig. 3, page 4, lines 32-36] a server subsystem as receiver sub system for secure biometric*), and

means for providing access to the controlled item dependent upon information in said secure access signal (*Hoffman, see [Col. 40, lines 62-67] the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]*), said method comprising the steps of:

receiving/code for receiving a biometric signal [*Martin, Page 4, lines 20-22*];

storing/code for storing the biometric signal received by the biometric sensor in the database as an administrator signature if the database of biometric signatures is empty (*Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists as empty, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14*);

code for, if an administrator signature has been stored in the database, classifying a legitimate sequence of biometric signals, each matching the administrator signature, as control information (*Koo, see the person having inputted his fingerprint is authorized as a new administrator [Page 16, lines 12-15]; and see also [Page 11, lines 16-18] the fingerprint code of the administrator is stored by receiving the code stored in the administration system*); and

performing/code for performing at least one of (a) amending information stored in the database depending upon the control information (*Koo, see [Page 17, lines 1-5] the door lock device recognizes a new user and erases all information related to the corresponding previous card key and changes as amended the initialization completion code*), and (b) classifying a subsequent biometric signal as one of an administrator signature and an ordinary signature depending upon the control information (*Koo, see [Page 16, lines 10-17, the fingerprint signature is registered as administrator and see also [Page 17, lines 22-25; 18/1-3] fingerprint code is registered as the initial user fingerprint code*).

One of ordinary skill in the art would have been motivated to incorporate the idea of enrolling biometric signatures into a database [*Hoffman, see [Col. 8, lines 35-40]* and providing access to the item based on accessibility attribute of Hoffman *[Col. 40, lines 62-67, Col. 41, lines 1-8]* within the system of Martin [*Fig. 4(a)-4(c)*] and the idea of Koo *[Page, 5, lines 19-22; Page 16, lines 8-10]* within the combined method of Martin and Hoffman [fig. 1] because the idea of Hoffman could provide the system of Martin the ability to an authorized user to alert authorities that a third party is coercing the user to request access without the third party being aware that an alert has been generated (*Hoffman, Col. 5, lines 62-67*) and the idea of Koo could provide the combined method of Hoffman and Martin an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (*Koo, Page 3, lines 21-23*).

Claims 50-51, 53-60 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffman in view of Koo.

Regarding claim 50, 51, Hoffman taught a method of/a computer program product having a computer program product recorded therein [*Hoffman, Col. 13, lines 51-60*] for directing a processor to execute a method for enrolling, by a transmitter sub-system [*Hoffman, Col. 12, lines*

50-55, Col. 13, lines 2-5, fig. 1 and 3], biometric signatures into a database of biometric signatures in a system for providing secure access to a controlled item (*see [Col. 8, lines 35-40] storage of the entered biometric sample from first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample*), the system comprising the transmitter sub-system and a receiver subsystem [*Fig. 3*] for providing access to the controlled item dependent upon an accessibility attribute received from the transmitter sub-system (*see [Col. 40, lines 62-67] the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]*);

Hoffman taught the method claim 50; Hoffman was silent on, said method comprising the steps of: storing/code for storing a biometric signal received by the transmitter sub-system in the database as an administrator signature; and enabling administrative processing of information stored in the database if a biometric signal matching the stored administrator signature is received by the transmitter.

However, Koo taught

storing/code for storing a biometric signal received by the transmitter sub-system in the database as an administrator signature (*Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14*); and

enabling/code for enabling administrative processing of information stored in the database if a biometric signal matching the stored administrator signature is received by the

transmitter (*Koo, see [Page 5, lines 19-22] upon receiving the fingerprint information of the administrator, the door lock device unlocks the door as administrative processing, if the received fingerprint information of the administrator coincides with any one of the stored fingerprint information of the administrator*).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the applicant's invention was made to modify the method of Hoffman with the teaching of Koo for storing biometric signal as an administrator signature and enabling administrative processing of information stored in the database if a biometric signal matching the stored administrator signature is received by the transmitter because they are analogous in biometric entry.

One of ordinary skilled in the art would have been motivated to incorporate the idea of Koo *[Page, 5, lines 19-22; Page 16, lines 8-10]* within the method of Hoffman [fig. 1] because the idea of Koo could provide the method of Hoffman to provide an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (*Koo, Page 3, lines 21-23*).

Regarding claim 53, the combination of Hoffman and Koo further taught a system according to claim 5, wherein the means for enrolling biometric signatures comprises:

means for determining if the database of biometric signatures is empty (*Koo, see [Page, 16, lines 5-9] the controller search the registered administrator fingerprint code information to see if there is no administrator fingerprint information exists as empty*); and

means for storing a biometric signal received by the biometric sensor in the database as an administrator signature if the database of biometric signatures is empty (*Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14*).

One of ordinary skilled in the art would have been motivated to incorporate the idea of Koo *[Page, 5, lines 19-22; Page 16, lines 8-10]* within the method of Hoffman [fig. 1] because the idea of Koo could provide the method of Hoffman to provide an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (*Koo, Page 3, lines 21-23*)

Regarding claim 54, the combination of Hoffman and Koo further taught a system according to claim 6, wherein the means for enrolling biometric signatures further comprises means for, if an administrator signature has been stored in the database, classifying a legitimate sequence of biometric signals, each matching the administrator signature, as control information (*Koo, see the person having inputted his fingerprint is authorized as a new administrator [Page 16, lines 12-15]; and see also [Page 11, lines 16-18] the fingerprint code of the administrator is stored by receiving the code stored in the administration system*).

Regarding claim 55, Hoffman in view of Koo further taught a system according to claim 7, wherein the means for enrolling biometric signatures further comprises means for determining if said sequence of biometric signals is legitimate dependent upon whether at least one of the number and duration of the signals are appropriate, and whether the signals are received within a predetermined time (*Hoffman, see [Col. 19, lines 16-35] the BIA continues to take new scans until <time> seconds pass. As time passes and snapshots of the print are taken and analyzed, if no print of appropriate quality is forthcoming, the BIA returns an error code of time expired. See also [Col. 19, lines 64-65], scanning terminates when either <time> number of seconds runs out, when the individual hits the "enter" key*).

Regarding claim 56, the combination of Hoffman and Koo further taught a system according to claim 7, wherein the means for enrolling biometric signatures further comprises

means for amending information stored in the database depending upon the control information (*Koo, see [Page 17, lines 1-5] the door lock device recognizes a new user and erases all information related to the corresponding previous card key and changes as amended the initialization completion code*).

Regarding claim 57, the combination of Hoffman and Koo further taught a system according to claim 7, wherein the means for enrolling biometric signatures further comprises means for classifying a subsequent biometric signal as one of an administrator signature and an ordinary signature depending upon the control information (*Koo, see [Page 16, lines 10-17, the fingerprint signature is registered as administrator and see also [Page 17, lines 22-25; 18/1-3] fingerprint code is registered as the initial user fingerprint code*).

Regarding claim 58, Hoffman in view of Koo further taught a system according to claim 1, wherein the transmitter sub-system is incorporated into at least one of (a) a remote control module comprising at least one of a key fob and a mobile communication device, and (b) an enclosure mounted next to the controlled item [*Hoffman, fig. 1, CATV, PPT, and fig. 2*].

Regarding claim 59, Hoffman in view of Koo further taught a system according to claim 6 further comprising means for providing a feedback signal for directing input of the control information (*Hoffman, see [Col. 19, lines 34-35, 42-43] the BIA returns an error code and display a message if fingerprint quality is not good or legitimate and responds with the success result code if print quality algorithm affirm the quality of scan*).

Regarding claim 60, Hoffman in view of Koo further taught a system according to claim 12, wherein the means for providing the feedback signal comprises at least one of a visual indicator and an audio indicator (*Hoffman, see [Col. 19, lines 35-36; fig. 3] the BIA display response on the LCD*).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MOHAMMAD L. RAHMAN whose telephone number is (571)270-7471. The examiner can normally be reached on IFP.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. L. R./
Examiner, Art Unit 2438
/Taghi T. Arani/
Supervisory Patent Examiner, Art Unit 2438